Protection Profile for a Wireless Local Area Network Network Interface Card and Access Point Summary

Agenda

- Purpose and Audience
- What is the Common Criteria?
- What are the benefits of being Common Criteria certified?
- What is a Protection Profile?
- Protection Profile Overview: Wireless Network Interface Card
- Protection Profile Overview: Access Point

Agenda (continued)

- Protection Profile Overview: Evaluation of Environmental Influence
- Protection Profile: Environmental Security Policies
- Summary
- Acronyms
- Useful CC Websites

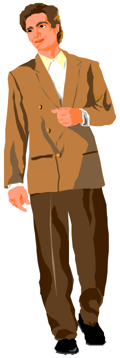
Purpose and Audience

- To explain the Common Criteria and its role in the IT world.
- To illustrate the benefits of being Common Criteria certified.
- To define the purpose of Protection Profiles.
- To present requirements presented by the NSA through the Protection Profiles for a WLAN Network Interface Card and an Access Point.
- To provide insight to vendors regarding requirements of a WLAN NIC and AP.

The Common Criteria is a multipart standard used for evaluation of IT products and systems.

- Provides a common set of requirements for evaluating the security of IT products and systems.
- Targets three groups that are considered to be principle users of the CC.

Consumer



Allows for comparability between functions of products and systems.

Vendor

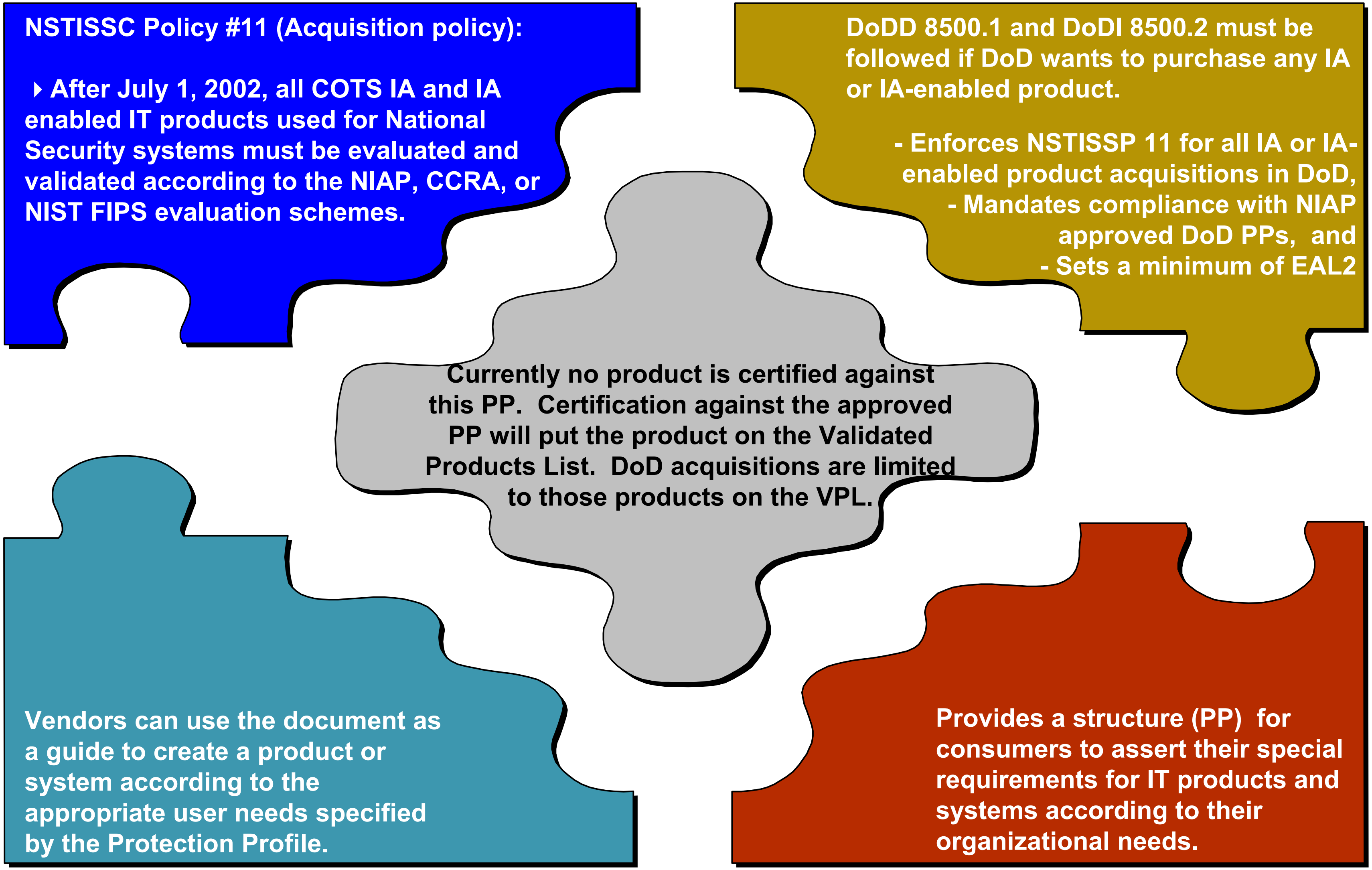
Provides security requirements to be satisfied by their products or systems.

Evaluator

Use criteria when determining if the product or system conforms to the security requirements for certification.

- CC is presented in three distinct parts which relate to the three targeted groups.
  - **Part 1**: Introduction and general concepts and principles of IT security evaluation
  - **Part 2**: Catalog of potential security functional requirements for Targets of Evaluations (TOEs) .
  - **Part 3**: Catalog of security assurance requirements;
    - -Establishes evaluation assurance levels (EALs) as a standard way of expressing the assurance requirements for TOEs;
    - -Defines evaluation criteria for Protection Profiles (PPs) and Security Targets (STs).

Why should the vendor care to be Common Criteria certified?



NSTISSC Policy #11 (Acquisition policy):

- After July 1, 2002, all COTS IA and IA enabled IT products used for National Security systems must be evaluated and validated according to the NIAP, CCRA, or NIST FIPS evaluation schemes.

DoDD 8500.1 and DoDI 8500.2 must be followed if DoD wants to purchase any IA or IA-enabled product.

- Enforces NSTISSP 11 for all IA or IA-enabled product acquisitions in DoD,
- Mandates compliance with NIAP approved DoD PPs, and
- Sets a minimum of EAL2

Currently no product is certified against this PP. Certification against the approved PP will put the product on the Validated Products List. DoD acquisitions are limited to those products on the VPL.

Vendors can use the document as a guide to create a product or system according to the appropriate user needs specified by the Protection Profile.

Provides a structure (PP) for consumers to assert their special requirements for IT products and systems according to their organizational needs.

What is a Protection Profile?

- Protection Profiles (PP) use the language of the Common Criteria in order to specify "What security functions I want as a user" in commercial off-the-shelf (COTS) IA or IA-enabled products to be used by the government.

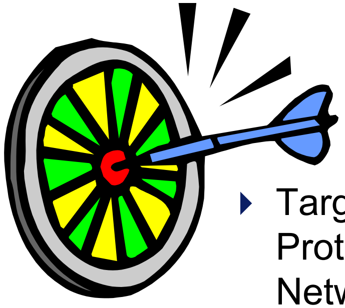
- Contents of PP include definitions of the security environment, assumptions, threats, objectives, and requirements for the product.

- Protection Profiles are not an endorsement of the product.

- Certificates issued according to a PP at EAL4 and below will be recognized by the United States, United Kingdom, Netherlands, France, Germany, Canada, Australia, and New Zealand.

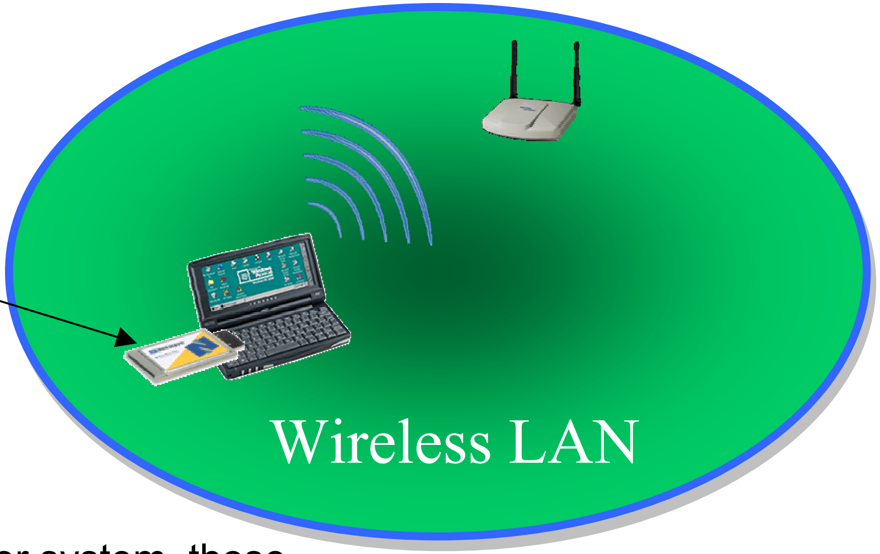
- Commercial testing laboratories certified by the National Information Assurance Partnership (NIAP) perform evaluations according to requirements specified in the ST and PP.

Protection Profile Overview: Wireless Network Interface Card



- Target of Evaluation (TOE) in this Protection Profile is a Wireless LAN Network Interface Card (NIC).

- The NIC will be a component of a larger system (i.e. Installed in a laptop.)



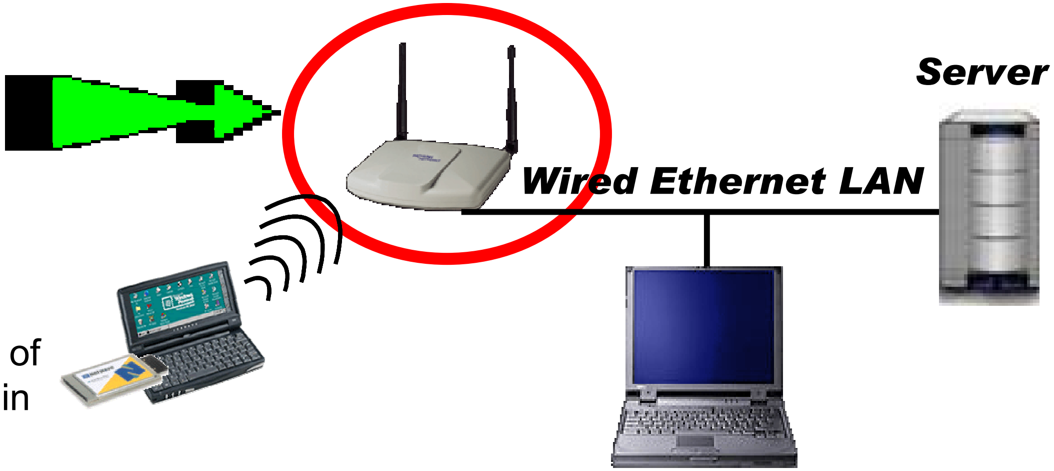
- Functional requirements of the TOE are:

  Administration: Because a NIC is part of larger system, those responsible for overseeing entire network are responsible for security of the card.

  Encryption: Requirements for providing cryptographic service must comply with Federal Information Processing Standard Publication (FIPS PUB) 140-2.

  Audit: WLAN administration will be responsible for storage and retrieval of audit events.

Protection Profile Overview: Access Point



- Target of Evaluation (TOE) in this Protection Profile is an Access Point (AP).

- The AP is an extension or replacement of of a wired network and allows for users to gain access to the network while mobile.

- Functional requirements of the TOE are:

Identification and Authentication (I&A): Administrators must be properly identified and authenticated by the TOE environment prior to performing any administrative tasks and accessing resources of the AP.

Administration: The AP only identifies one administrative role which will be assigned to those responsible for installation, configuration, and maintenance of the AP.

Information Flow Control: An encrypted communications channel is required of the TOE environment so that the AP may enforce information flow control.

Encryption: Requirements for providing cryptographic service must comply with Federal Information Processing Standard Publication (FIPS PUB) 140-2.

Audit: WLAN administration will be responsible for storage and retrieval of audit events.

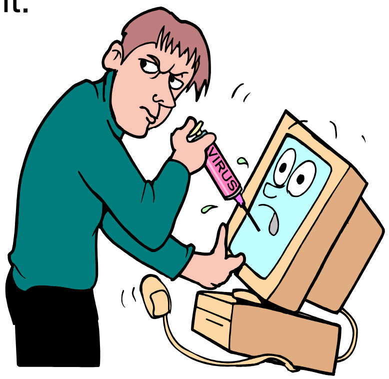
Protection Profile Overview: Evaluates Environmental Influence from Assumptions and Threats to Security

Secure Usage Assumptions

- Presents events presumed to occur from a source other than the NIC and AP.
- In the basic robustness level security environment the NIC and AP must address threats and policies identified.
- Physical security will be provided by the IT environment itself.
- Administrators must follow appropriate guidelines.

Threats to Security

- Threats are determined by motivation, expertise, and available resources of the individual.
- WLANs propose threats due to exposure based on RF transmission of information.
- Susceptible to passive and active attacks.
- PP provides numerous threats addressed by the NIC and AP itself and by the operating environment.

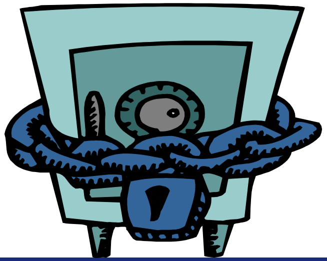


Protection Profile Overview: Security Environment Policies

- A WLAN NIC and AP must meet security requirements for a Basic Level of Security.
- The PP lists rules, practices, and procedures imposed by the organization for its security needs.
- Policies cover user accountability.
- Cryptography must be FIPS compliant.
- Usage must comply with the DoD Wireless Policy.
- The PP identifies objectives that counter previously introduced threats.
- Security must be addressed by the environment in which the NIC operates and by non-technical factors.

Summary

- Common Criteria is an essential means of communication for consumers and evaluators to assess security requirements of IT products, and provides a mechanism for vendors to communicate security functionality for IT products.
- Protection Profiles offer a mutual ground for communicating specific functions, requirements, and objectives desired by the National Information Assurance Partnership.
- Products and systems must be CC certified against the PP to be recognized in the DoD market.
- A NIC and AP must substantiate a Basic Robustness Level of Security because of its role in the IT environment.
- Threats, assumptions, and policies pertaining to the IT environment govern the design and implementation of security for a WLAN NIC and AP.



Acronyms

AP	Access Point
CC	Common Criteria
COTS	Commercial Off-the-Shelf
DoD	Department of Defense
FIPS PUB	Federal Information Processing Standard Publication
I&A	Identification and Authentication
IT	Information Technology
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NSA	National Security Agency
NSTISSC	National Security Telecommunications and Information Systems Security Committee
PP	Protection Profile
RF	Radio Frequency
TOE	Target of Evaluation
ST	Security Target
WLAN	Wireless Local Area Network

Useful CC Web Sites

- General info:
  - NSTISSP #11

    http://www.nstissc.gov/Assets/pdf/nstissp_11.pdf

    http://niap.nist.gov/cc-scheme/nstissp-faqs.html
  - NIAP homepage:

    http://niap.nist.gov/
  - Common Criteria

    http://www.commoncriteria.org

- Validated vendor evaluation claims:
  - US CCEVS validated products list:

    Link located at http://niap.nist.gov/cc-scheme/index.html
  - FIPS-140 validated products list

    http://csrc.nist.gov/cryptval/140-1/1401val.htm
  - UK certified products list:

    http://www.cesg.gov.uk/assurance/iacs/itsec/cpl/index.asp